ID: 483659
Sample Name:
HSBc20210216B1.exe
Cookbook: default.jbs
Time: 11:04:40
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

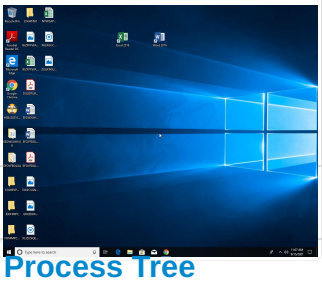
Windows Analysis Report HSBc20210216B1.exe

Overview

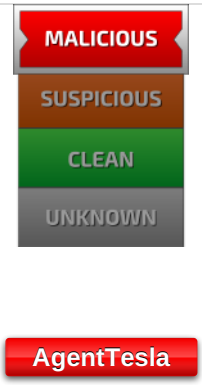
General Information

Sample Name:	HSBc20210216B1.exe
Analysis ID:	483659
MD5:	ced0f1b2afd1d48..
SHA1:	d999697f2b1111b.
SHA256:	8bd91aa543ff97c..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



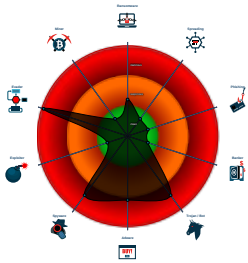
AgentTesla

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Sigma detected: Bad Opsec Default…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- HSBc20210216B1.exe (PID: 6404 cmdline: 'C:\Users\user\Desktop\HSBc20210216B1.exe' MD5: CED0F1B2AFD1D48ECB5DC8A563C836C9)
  - RegSvcs.exe (PID: 6648 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- NXLun.exe (PID: 6692 cmdline: 'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 4088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- NXLun.exe (PID: 6780 cmdline: 'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6832 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "paola.micheli@copangroup.xyz",
  "Password": "gibson.1990",
  "Host": "us2.smtp.mailhostbox.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.490503848.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.490503848.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.249871977.000000000301000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.251226749.000000000409000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.251226749.000000000406 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.HSBc20210216B1.exe.412acb8.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.HSBc20210216B1.exe.412acb8.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.HSBc20210216B1.exe.412acb8.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

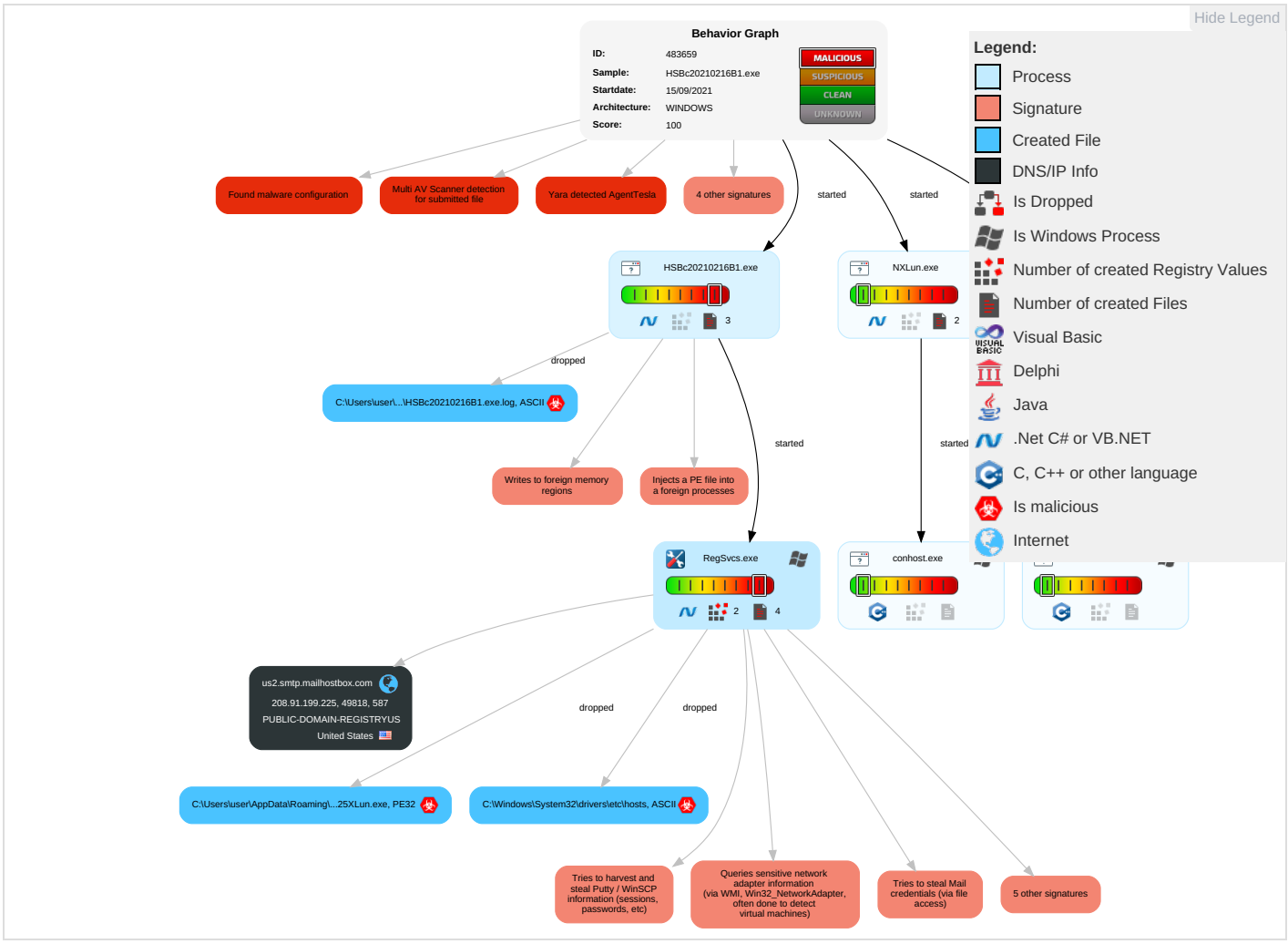
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 2 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	Credentials in Registry 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 2 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol

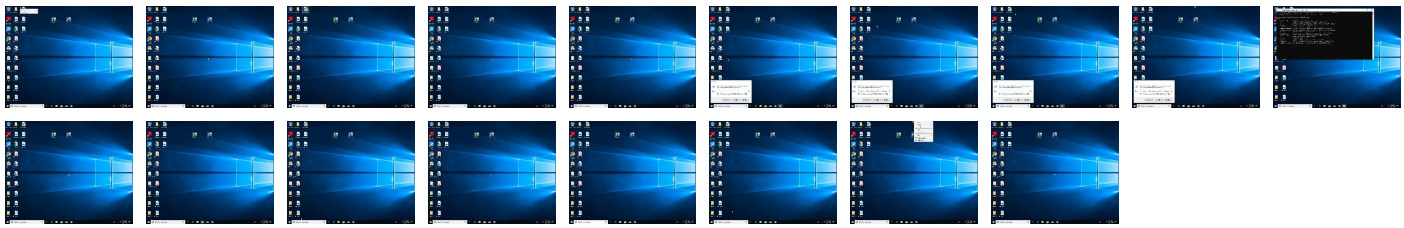
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
HSBc20210216B1.exe	21%	Virustotal		Browse
HSBc20210216B1.exe	17%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\NXLun\NXLun.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\NXLun\NXLun.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comB4	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comnv	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/3	0%	Avira URL Cloud	safe	
http://www.carterandcone.com3	0%	Avira URL Cloud	safe	
http://www.carterandcone.comvw	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t-u	0%	Avira URL Cloud	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.carterandcone.com.12.p	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnM4	0%	Avira URL Cloud	safe	
http://www.carterandcone.comIyU4	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/N	0%	Avira URL Cloud	safe	
http://5c3LgjsgKO5q1r.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.carterandcone.comBv	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.com-y	0%	Avira URL Cloud	safe	
http://www.carterandcone.comcRyJ4	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cne4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/E	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/D	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/x	0%	URL Reputation	safe	
http://jdPkJL.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/;	0%	URL Reputation	safe	
http://www.fontbureau.comceto	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.carterandcone.comjw	0%	Avira URL Cloud	safe	
http://www.carterandcone.comw	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/adnl	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://www.carterandcone.comTCwy	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFn	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.225	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.225	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483659
Start date:	15.09.2021
Start time:	11:04:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HSBc20210216B1.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@7/6@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 80.1% • Quality standard deviation: 17.2%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:05:47	API Interceptor	1x Sleep call for process: HSBc20210216B1.exe modified
11:06:00	API Interceptor	731x Sleep call for process: RegSvcs.exe modified
11:06:10	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run NXLun C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
11:06:18	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run NXLun C:\Users\user\AppData\Roaming\NXLun\NXLun.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.225	POINQUIRYRFQ676889.exe	Get hash	malicious	Browse	
	qiQvJ3jGU2.exe	Get hash	malicious	Browse	
	S121093 - RE Wire Transfer - 8,000.00 USD - deposit.exe	Get hash	malicious	Browse	
	RFQ#MAT#Quotation No. 20077253.exe	Get hash	malicious	Browse	
	Payment Advice 09092021 HSBC096754BK56CBREF.exe	Get hash	malicious	Browse	
	PaymentReceipt.doc	Get hash	malicious	Browse	
	Swift Transfer Copy mt103_PDF.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.MachineLearning.Anomalous.94.8891.exe	Get hash	malicious	Browse	
	PURCHASE ORDER 2021.exe	Get hash	malicious	Browse	
	L9d4ISc9LF4Yv1t.exe	Get hash	malicious	Browse	
	P.O_345.exe	Get hash	malicious	Browse	
	revised order-number 3A6.exe	Get hash	malicious	Browse	
	QUOTATION -PDF-SCAN-COPY.exe	Get hash	malicious	Browse	
	Urgent RFQ #2105031.pdf.exe	Get hash	malicious	Browse	
	Listed Items Order.exe	Get hash	malicious	Browse	
	order-2021-PO # 0834.xlsx	Get hash	malicious	Browse	
	qPlRnI13fW.exe	Get hash	malicious	Browse	
	PO.exe	Get hash	malicious	Browse	
	VOn3J2hVHa.exe	Get hash	malicious	Browse	
	BANK REPORT AUTHORIZATION LETTER.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	POINQUIRYRFQ676889.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO- 45020032 Juv#U00e9l AS.exe	Get hash	malicious	Browse	• 208.91.199.224
	48q74tT5IK.exe	Get hash	malicious	Browse	• 208.91.199.224
	qiQvJ3jGU2.exe	Get hash	malicious	Browse	• 208.91.199.225
	S121093 - RE Wire Transfer - 8,000.00 USD - deposit.exe	Get hash	malicious	Browse	• 208.91.199.224
	Final Sept Order #0921.exe	Get hash	malicious	Browse	• 208.91.199.224
	DHL Express Invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	ee5s192YZ34Ybve.exe	Get hash	malicious	Browse	• 208.91.199.223
	Payment Advice 09092021 HSBC096754BK56CBREF.exe	Get hash	malicious	Browse	• 208.91.199.224
	sapa list.doc	Get hash	malicious	Browse	• 208.91.198.143
	RFQ#MAT#Quotation No. 20077253.exe	Get hash	malicious	Browse	• 208.91.199.225
	04142021_10RD0207S0N0000,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	HY19071 PI.exe	Get hash	malicious	Browse	• 208.91.198.143
	PO_Contract_ANR07152112_20210715181907__110.exe	Get hash	malicious	Browse	• 208.91.198.143
	RFQ-#80986-3580.exe	Get hash	malicious	Browse	• 208.91.199.224
	Bank swift copy.exe	Get hash	malicious	Browse	• 208.91.199.224
	i9fnXDoul7.exe	Get hash	malicious	Browse	• 208.91.199.225
	Shipping Doc_968018592077_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	AWB_968018592077_Invoice_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	#QuotationEX-2-0093-Q-FOB@2021-10-09.exe	Get hash	malicious	Browse	• 208.91.199.224

ASN

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	POINQUIRYRFQ676889.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO- 45020032 Juv#U00e9l AS.exe	Get hash	malicious	Browse	• 208.91.199.224
	Qoutation for Strips.doc	Get hash	malicious	Browse	• 162.215.241.145
	48q74tT5IK.exe	Get hash	malicious	Browse	• 208.91.199.224
	qiQvJ3jGU2.exe	Get hash	malicious	Browse	• 208.91.199.225
	S121093 - RE Wire Transfer - 8,000.00 USD - deposit.exe	Get hash	malicious	Browse	• 208.91.199.224
	angelzx.exe	Get hash	malicious	Browse	• 162.215.241.145
	Final Sept Order #0921.exe	Get hash	malicious	Browse	• 208.91.199.224
	PO KV18RE001-A5193.doc	Get hash	malicious	Browse	• 199.79.62.16
	DHL Express Invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	0zWKZlSOqL.exe	Get hash	malicious	Browse	• 199.79.62.16
	ee5s192YZ34Ybve.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment advice_103.exe	Get hash	malicious	Browse	• 199.79.62.145
	QUOTATION.exe	Get hash	malicious	Browse	• 162.215.249.19
	diagram-595.doc	Get hash	malicious	Browse	• 116.206.105.115
	Payment Advice 09092021 HSBC096754BK56CBREF.exe	Get hash	malicious	Browse	• 208.91.199.224
	LJUNGBY QUOTATION.doc	Get hash	malicious	Browse	• 162.215.241.145
	TPL020321.doc	Get hash	malicious	Browse	• 162.215.241.145
	sapa list.doc	Get hash	malicious	Browse	• 208.91.198.143
	diagram-378.doc	Get hash	malicious	Browse	• 116.206.105.115

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\NXLun\NXLun.exe	SOA for V.R at USD.exe	Get hash	malicious	Browse	
	required.exe	Get hash	malicious	Browse	
	Bank details.exe	Get hash	malicious	Browse	
	Payment Advice_JPEG.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	pleas.exe	Get hash	malicious	Browse	
	MHHHG_9847654673T3RDNVAASGU.NET.exe	Get hash	malicious	Browse	
	70654 SSEBACT.exe	Get hash	malicious	Browse	
	AUG. SOA -USD53,123.16.exe	Get hash	malicious	Browse	
	Yingtron Miga Trading - Request for Quotation.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.BackDoor.SpyBotNET.25.7070.exe	Get hash	malicious	Browse	
	PO_Contract_ANR07152112_20210715181907__110.exe	Get hash	malicious	Browse	
	TWM#U007e-04987474848GRRT.exe	Get hash	malicious	Browse	
	OA9862qYq7.exe	Get hash	malicious	Browse	
	PO#-BRU-2020-0010.exe	Get hash	malicious	Browse	
	PO 901103237.exe	Get hash	malicious	Browse	
	s8uDIcv0XT.exe	Get hash	malicious	Browse	
	Bank Payment Transfer for PI. BT-GJ21001.exe	Get hash	malicious	Browse	
	TT- Swift Copy.exe	Get hash	malicious	Browse	
	323-TG-0653.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HSBc20210216B1.exe.log

Process:	C:\Users\user\Desktop\HSBc20210216B1.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HSBc20210216B1.exe.log	
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NXLun.exe.log	
Process:	C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Roaming\NXLun\NXLun.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D(B42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Roaming\NXLun\NXLun.exe	
Joe Sandbox View:	• Filename: SOA for V.R at USD.exe, Detection: malicious, Browse • Filename: required.exe, Detection: malicious, Browse • Filename: Bank details.exe, Detection: malicious, Browse • Filename: Payment Advice_JPEG.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: pleas.exe, Detection: malicious, Browse • Filename: MHHHG_9847654673T3RDNVAASGU.NET.exe, Detection: malicious, Browse • Filename: 70654 SSEBACT.exe, Detection: malicious, Browse • Filename: AUG. SOA -USD53,123.16.exe, Detection: malicious, Browse • Filename: Yingtron Miga Trading - Request for Quotation.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.BackDoor.SpyBotNET.25.7070.exe, Detection: malicious, Browse • Filename: PO_Contract_ANR07152112_20210715181907__110.exe, Detection: malicious, Browse • Filename: TWM#U007e-04987474848GRRT.exe, Detection: malicious, Browse • Filename: OA9862qYq7.exe, Detection: malicious, Browse • Filename: PO#-BRU-2020-0010.exe, Detection: malicious, Browse • Filename: PO 901103237.exe, Detection: malicious, Browse • Filename: s8uDIcv0XT.exe, Detection: malicious, Browse • Filename: Bank Payment Transfer for PI. BT-GJ21001.exe, Detection: malicious, Browse • Filename: TT- Swift Copy.exe, Detection: malicious, Browse • Filename: 323-TG-0653.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]...

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Preview:	..127.0.0.1

\Device\ConDrv	
Process:	C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assemb ly, for MS Windows

General

Entropy (8bit):	7.7208885042844395
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	HSBc20210216B1.exe
File size:	673280
MD5:	ced0f1b2afd1d48ecb5dc8a563c836c9
SHA1:	d999697f2b1111b7b72603bc9bee04cbf7a3664c
SHA256:	8bd91aa543ff97c07aae2a257ea7f97729c4345be8c4c4e6dea2e1aa48324bc3
SHA512:	40e38ba780d4e5ef665ce3b9130eb1552683f2e93618ee54c9ab9373d30d2dbcd2b68520a40c4f063fb9f9f74dafdc97baf1b0517adb6ee4548f0f5ecde25902
SSDEEP:	12288:nc2I/yzQs2TaIpI1KJAHSQNEMePF4AabmOil3rXiELMExnifxSIW:8MIpI1KJAHD64sGEkwIW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...~.Aa.....n.....z.... ....@.. .....@.....

File Icon

Icon Hash:	f1f0f4d0eecccc71

Static PE Info

General

Entrypoint:	0x49f47a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6141947E [Wed Sep 15 06:36:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x9d480	0x9d600	False	0.87101928614	data	7.79300898434	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0xa0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0xa2000	0x6b74	0x6c00	False	0.44165943287	data	5.12878842181	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 11:07:24.976735115 CEST	192.168.2.3	8.8.8.8	0x76ca	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 11:07:25.005244970 CEST	8.8.8.8	192.168.2.3	0x76ca	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Sep 15, 2021 11:07:25.005244970 CEST	8.8.8.8	192.168.2.3	0x76ca	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Sep 15, 2021 11:07:25.005244970 CEST	8.8.8.8	192.168.2.3	0x76ca	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Sep 15, 2021 11:07:25.005244970 CEST	8.8.8.8	192.168.2.3	0x76ca	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Sep 15, 2021 11:07:25.390908003 CEST	587	49818	208.91.199.225	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Sep 15, 2021 11:07:25.391247988 CEST	49818	587	192.168.2.3	208.91.199.225	EHLO 358075
Sep 15, 2021 11:07:25.541528940 CEST	587	49818	208.91.199.225	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Sep 15, 2021 11:07:25.541909933 CEST	49818	587	192.168.2.3	208.91.199.225	STARTTLS
Sep 15, 2021 11:07:25.691804886 CEST	587	49818	208.91.199.225	192.168.2.3	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: HSBc20210216B1.exe PID: 6404 Parent PID: 996

General

Start time:	11:05:38
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\HSBc20210216B1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\HSBc20210216B1.exe'
Imagebase:	0xd60000
File size:	673280 bytes
MD5 hash:	CED0F1B2AFD1D48ECB5DC8A563C836C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.249871977.0000000003061000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.251226749.0000000004069000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.251226749.0000000004069000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.252492077.00000000042C5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.252492077.00000000042C5000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 6648 Parent PID: 6404

General

Start time:	11:05:49
Start date:	15/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x480000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.490503848.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.490503848.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.494922031.00000000026E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.494922031.00000000026E1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: NXLun.exe PID: 6692 Parent PID: 3388

General

Start time:	11:06:19
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe'
Imagebase:	0xa90000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 4088 Parent PID: 6692

General

Start time:	11:06:19
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: NXLun.exe PID: 6780 Parent PID: 3388

General

Start time:	11:06:27
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe'
Imagebase:	0xc50000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Written

File Read

Analysis Process: conhost.exe PID: 6832 Parent PID: 6780

General

Start time:	11:06:27
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis